AWS Guidelines

1. **Secure your Password and Access key:**

   The two main types of credentials used for **accessing your account** are **Password** and **Secret/Access key**.
   You should safeguard passwords and access keys as you would any other confidential personal data, and never embed them in publicly accessible code (i.e. a public Git repository). For added security, frequently rotate or update all security credentials.
   Note:
   - Please do not share your access key & Secret to anyone and anywhere.
   - **IMP**- Please do not put your access key and secret key to any public repository like Github, Bitbucket etc.
   - Delete the access key and secret key once your project is completed.
   - If you suspect that a password or access key pair has been exposed, immediately rotate and delete the exposed credentials.

2**. Cost Optimization:**

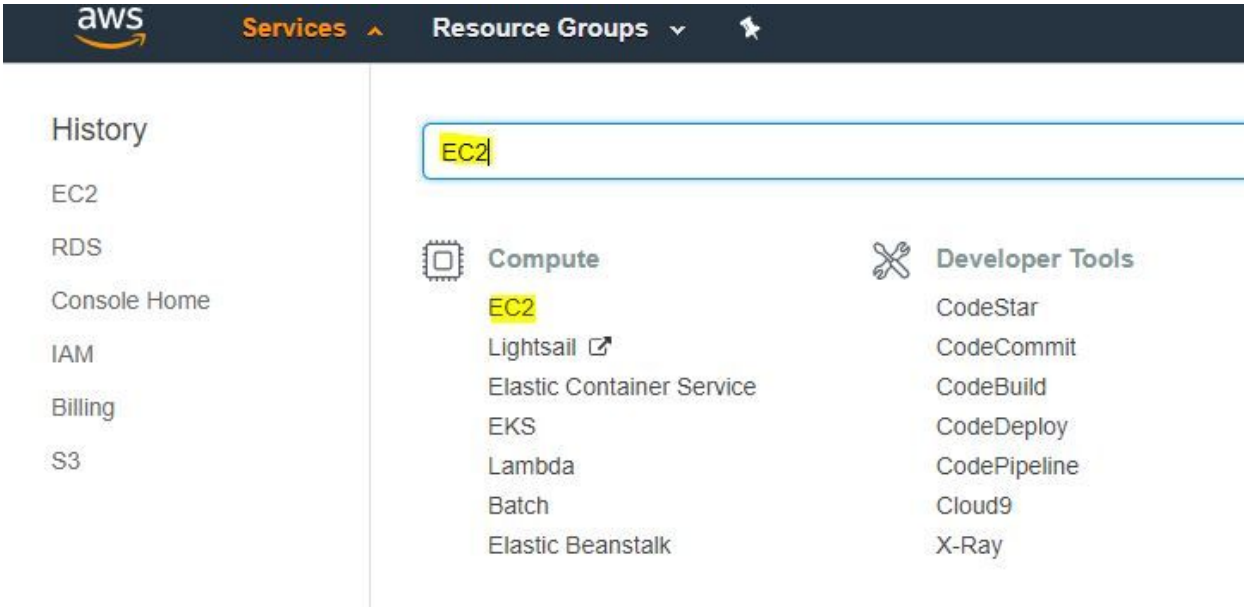
   - Please use the same region for creating all the AWS services.
   - We will be using the N.Virginia region as it is cheapest, and we would suggest you to use the N.Virginia region to avoid any confusion

3. **Complete the deployment process within a day:**
   - We strictly advise you to complete the whole deployment by following the lab manual within a day. In extreme case, if you run into some problem or you are not able to do so, stop all the instances before logging out of the AWS Console dashboard.

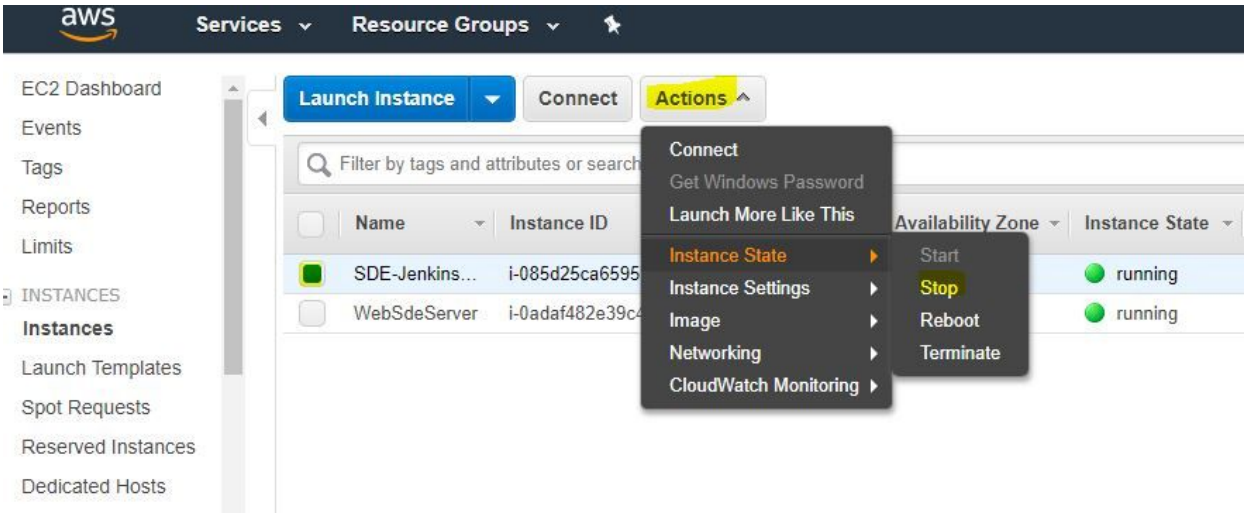
4. **Terminate AWS services:**
   - Once your project deployment is completed successfully then terminate the EC2 Instance, RDS instance and S3 bucket and CloudWatch service.

5. **Steps to stop and start AWS Services such as EC2 and RDS**:
   - **Stop EC2 instance:**

1. Navigate to EC2 service in AWS

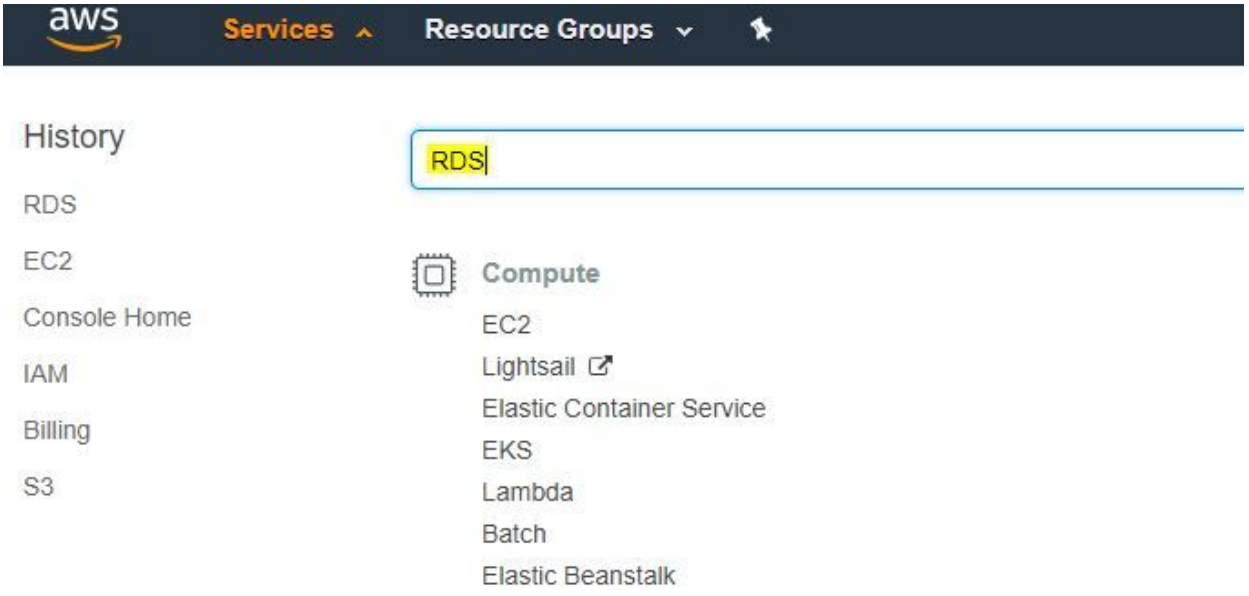


2. Select the EC2 instance you want to stop> Click on Actions> Click on Stop

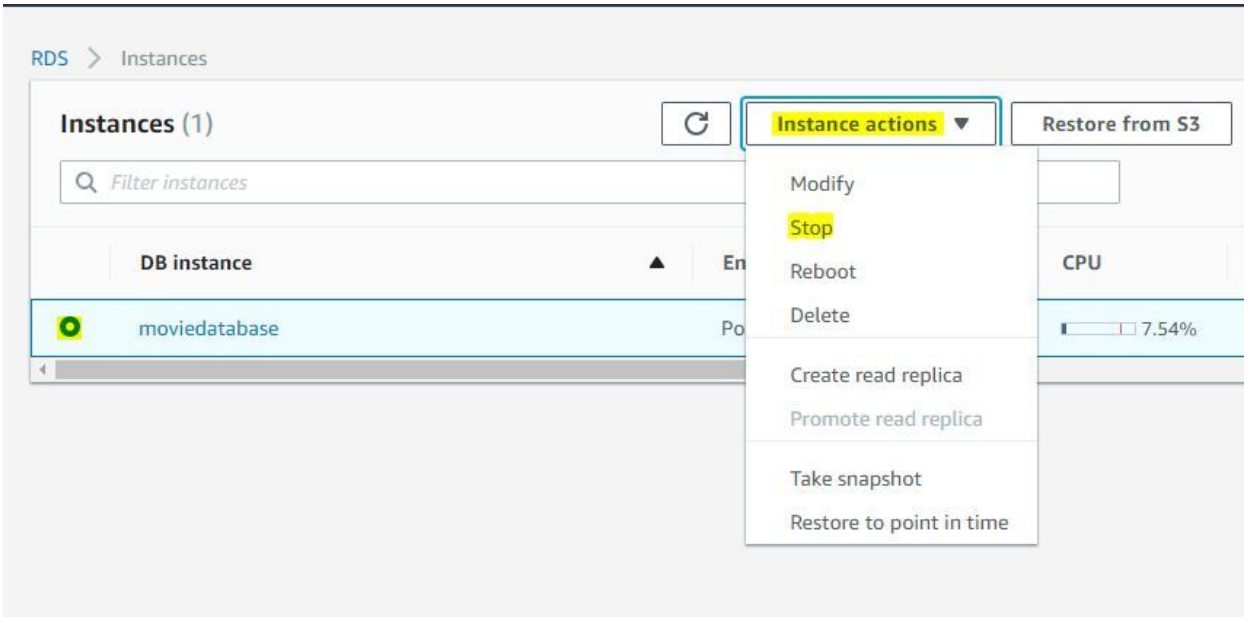


- **Stop RDS Instance:**

1. Navigate to RDS Service in AWS:

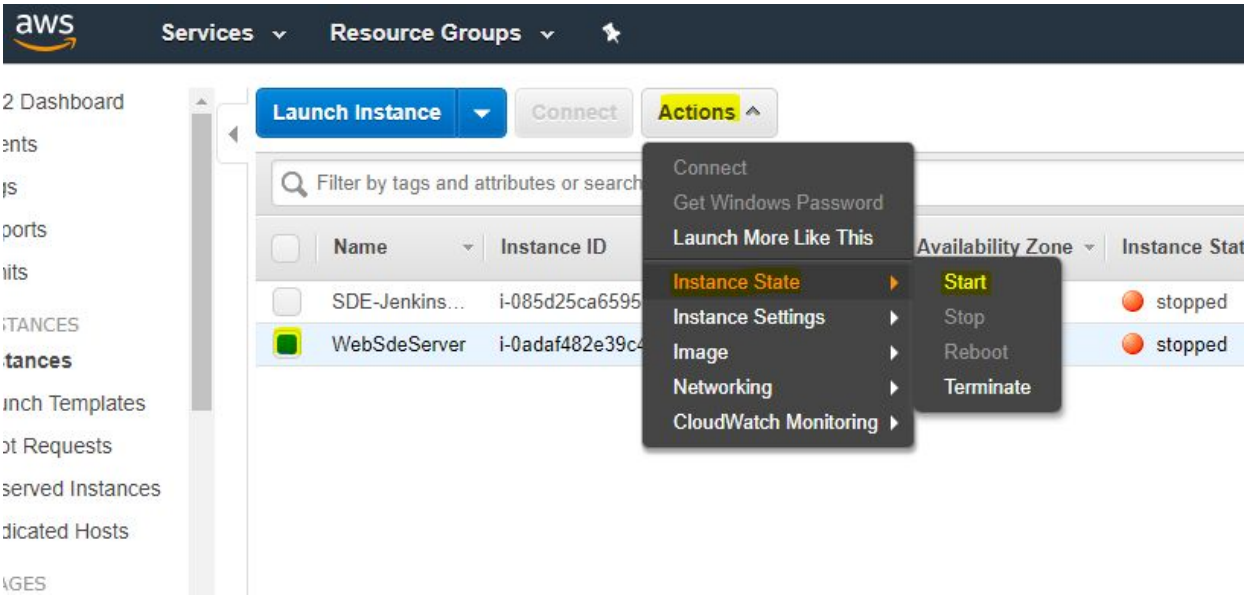


2. Select the RDS instance you want to Stop> Click on Instance actions> Click on Stop> Select No in Create Snapshot:



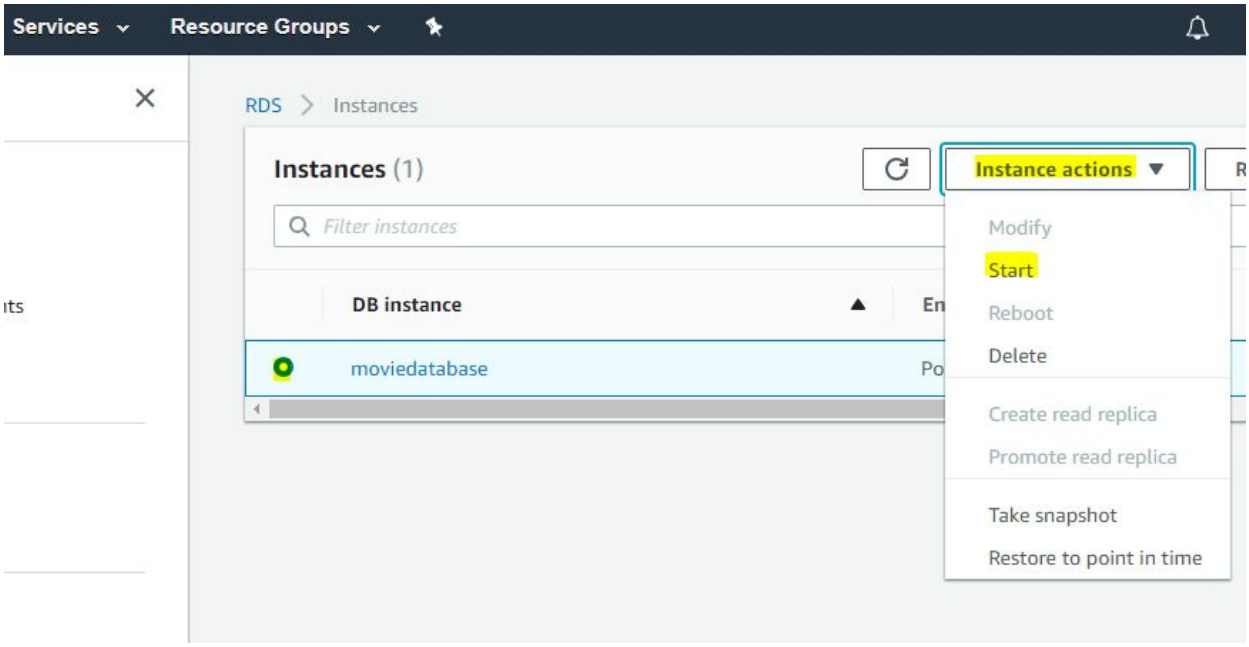
7. **Starting AWS services such as EC2 and RDS**
    - **Start EC2 instance**

1. Select the EC2 instance you want to start> Click on Actions> Click on Start:



- **Start RDS Instance**

2. Select the RDS instance you want to start> Click on Instance actions> Click on Start:



8. **Public IP change:**
   - Whenever you stop and restart any EC2 instance **public IP address of that instance changes**. You have used this public IP address in both Jenkins and GitHub. So, you need to communicate the updated IP address to both Github and Jenkins.
   - **These are the steps to update the public IP address.**

- In the Frontend repository in Github, open this file ‘src/screens/Controller.js’. Click on the edit button and replace the IP address inside the constructor() with the new IP of the web server.
- In the Frontend repository in Github open Settings> click Webhooks> delete the existing webhook> click Add webhooks> Enter the payload URL with the new IP address of the Jenkins server> Click Add webhooks.
- In the Backend repository in Github open Settings> click Webhooks> delete the existing webhook> click Add webhooks> Enter the payload URL with the new IP address of the Jenkins server> Click Add webhooks.
- Open Jenkins with new public IP> Click Manage Jenkins> Click Configure System> Scroll down to Jenkins Location> Update the Jenkins URL
- Open Jenkins with new public IP> Click Manage Jenkins> Click Configure System> Scroll down to Publish over SSH plugin> Inside SSH Servers> Hostname> Update the new IP address of web server.